A Study on Diagnosabilit y of Space Station ECLSS

S. Padalkar, W. Blokland, and J. Sztipanovits
Vanderbilt University. Nashville, TN.

ABSTRACT

This research demonstrates the use of the Multigraph Architecture (MGA) for studies on the Environment Control and Life Support System (ECLSS). The objective of this effort has been the following: (1) to create an updated set of models of the Potable Water Subsystem (PWS) by using the graphical model building tools of the Multigraph Programming Environment (MPE), (2) to derive a real-time alarm simulator from the models, and (3) to demonstrate the effects of sensor allocation on the diagnosability of the PWS. This work may serve as a preliminary study for the detailed analysis of the sensor allocation and diagnosability problems in the ECLSS.

PROBLEM STATEMENT

Real-time monitoring and diagnostics is a necessary component of critical and complex systems such as ECLSS. Their task is to provide an extensive fault detection capability combined with diagnostics of reasonable depth. The function of ECLSS requires the diagnostic system to operate continuously in a dynamically changing environment. Diagnostic hypotheses must be generated in an evolving fault scenario so as to allow corrective measures that can prevent the development of catastrophic failures.

Construction of real-time diagnostic systems is not straightforward. The diagnostic reasoning is subject to time constraints, has to indicate modeling errors, and must be robust enough to handle sensor failures. In dynamic systems where the presence of feedback loops are inevitable, the diagnostic system must apply temporal reasoning. These and similar requirements make the application of "associative" approaches - that associate patterns of observations (symptoms) with the underlying causes - unfeasible [1].

Model-based approaches have the potential of solving the challenging problems of real-time diagnostics. Core components of model-based diagnostic systems are: (1) well defined model of the system to be diagnosed, and (2) diagnostic reasoning algorithm, which interprets the observations in the context of the model. The purpose of the observations is to detect anomalies in the system behavior. Fault detection algorithms use the incoming data from sensors that are allocated in the plant and process them to check whether various operational constraints are satisfied.

Performance of a particular diagnostic system depends on the number and reliability of sensors providing input data for the fault detection system. Having a large number of reliable sensors "close" to the possible fault sources makes the diagnostic reasoning simple and the result accurate. The obvious limitation in improving the diagnostic performance by increasing the number of sensors is cost. Sensors are usually scarce resources that have to be carefully allocated. A realistic design approach can not be based on the unlimited availability of these resources. On the contrary, the question is how to allocate a limited number of sensors of limited reliability so as to achieve the best diagnostic resolution?

The objectives of this study have been to create models for the fault diagnostic system of PWS, to use the models for simulating real-time alarm sequences, and to demonstrate the relationship between sensor allocation and diagnostic resolution.

MULTIGRAPH ARCHITECTURE

Over the last five years Vanderbilt has developed a technology for the design and implementation of model-based real-time systems. The basic principles used in the construction of the Multigraph Architecture (MGA) are the followings:

- Model-based systems include: (1) multiple-aspect models of the system to be monitored, controlled, and diagnosed, (2) models of the components of the monitoring, control, and diagnostic system itself, and (3) models of their interaction.
- The models form a new level of abstraction in the system architecture, and are actively involved in the system operation.
- Driven by the external events that are received by the system, the models are continuously interpreted and reinterpreted. Interpretation of the models of the monitoring/control/diagnostic system components generates their actual implementation on a lower level. The lower level implementations determine the actual behavior of the system at a given time. Therefore, a model-based system can dynamically change its behavior if the state of the model changes on a higher level. This is one of the ultimate advantages of the model-based approach. It provides a very high-level of flexibility in a very simple manner.
- Most of the complexity of the model-based system is concentrated on the models. The rest of the system is a set of very generic, highly "reusable" procedural code providing the run-time support for the system. Due to this, the development technology of model-based systems can be supported by extremely efficient graphical model building, and automatic model verification tools.

The Multigraph Architecture (MGA) includes two main components, a graphic programming environment (Multigraph Programming Environment, MPE) [2] and a parallel execution environment (Multigraph Execution Environment, MEE) [3]. MPE facilitates building and maintaining multiple-aspect models of heterogeneous systems. The iconic graphic editors of MPE represent models in the form of graphic pictures and generate their symbolic representation in terms of specific declarative languages. MEE is a macro-dataflow model, which provides a unified environment for the execution of the functional components of model-based systems. Important feature of the Multigraph technology is that executable systems are automatically generated from the models, providing very high level software productivity.

MODELING TECHNIQUE

Any complex electro-mechanical system such as the ECLSS can be viewed from many different aspects. One such aspect is its function, another is its structure. A hierarchical decomposition of the functional aspect yields the Hierarchical Functional Model (HFM). Similarly, a hierarchical decomposition of the structural aspect yields the Hierarchical Component Model (HCM). The Hierarchical Fault Model (HFaM) is derived in the context of the HFM and the HCM.

Hierarchical Functional Model

The individual nodes in the HFM are referred to as processes. A process in the HFM can be thought of as an abstract entity that performs a specific function. It is possible to model certain viewpoints of every process. They are the structural viewpoint and the failure propagation viewpoint.

Structural Viewpoint

The structural viewpoint of a process represents information about its internal structure. The following items are acquired for each process:

- **Input/Output Process Variables**,
- **Process States**,
- **Alarms**, and
- **Subprocesses**.

Failure Propagation Viewpoint

While performing its function, a process may violate some of its functional constraints due to the presence of faults. When such a violation occurs, the process is said to contain a failure-mode. The presence of a failure-mode can be detected by an alarm derived from a sensor associated with the process. A process can exist in a number of different states. The following items are acquired for each process:

- **Failure-modes**.
- **Failure-mode Alarm associations**. Each failure-mode alarm association has associated with itself, the list of process states in which it is active.
- A **fault propagation graph** (FPG). The FPG of a process denotes a causal relationship between its failure-modes and the failure-modes of its subprocesses. Each causal link in the FPG originates from a failure-mode of a subprocess and propagates to a failure-mode of either a subprocess or the parent. A causal link is weighted by four parameters, the fault propagation probability, the minimum fault propagation time, the maximum fault propagation time, and the list of process states in which the link is active. An AND type of causal link is also permitted in the FPG. This link has as ancestors, more than one subprocess failure-mode, and as destination more than one subprocess failure-mode and/or parent failure-mode. In case of the AND type of causal link, the fault propagation probability implies the probability of occurrence of the destination failure-modes after all the ancestor failure-modes have occurred. Similarly, the minimum and maximum fault propagation times are the minimum and maximum times during which the destination failure-modes will occur after all ancestor failure-modes have occurred.

Hierarchical Component Model

A component in the HCM is an actual piece of hardware that can assist a variety of processes in performing their functions. The source of faults in a system are any of the components in the HCM. Each component upon becoming faulty, can exhibit a number of failed-states. The following items are acquired for each component:

- **Component failed-states** and
- **Subcomponents**.

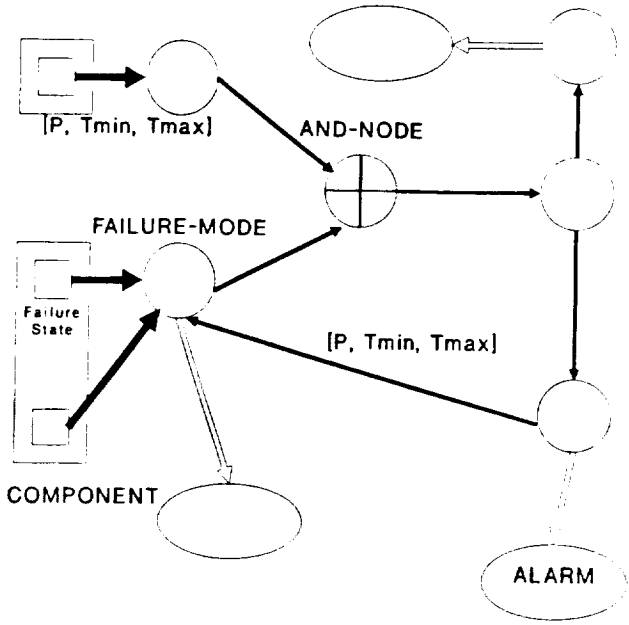

Figure 1: Process fault model

Function-Component Interactions

A failed-state in a component can lead to a number failure-modes being present in some of the processes in the HFM. The set of causal relationships between the failed-states of the components, and the failure-modes of the processes, is acquired. A causal link is weighted by three parameters, the fault propagation probability, the minimum fault propagation time, and the maximum fault propagation time.

Hierarchical Fault Model

The fault model of a process is the fault propagation viewpoint of the process model, and the set of causal links between the component failed-states and the process' failure-modes and failure-modes of all the process' existing subprocesses. The HFaM is the collection of all such process fault models. An example of a process fault model is shown in Figure 1.

REASONING TECHNIQUE

The occurrence of a fault in the system implies that a component or a set of components exhibit failed-states. The existence of failed-states leads to the existence of failure-modes in some processes. Among the set of existing failure-modes, those with associated alarms are detected by the ringing of those alarms. These ringing alarms start the diagnostic activity. The diagnostic reasoning technique selects the highest process in the HFM containing ringing alarms, and runs a Faulty Component Identification Algorithm (FCIA) on the fault model of the process' parent. The FCIA back-propagates along the ringing alarm failure-modes, and using structural and temporal constraints, identifies a set of possible fault source components [4]. The FCIA is guaranteed to produce a result in real-time because it possesses a polynomial time complexity. This time complexity is $O(n^3)$, where n is the number of existing failure-modes in the FPG of that process.

Certain factors affect the number of fault source candidates identified by the FCIA. A single fault case is where one component is responsible for the failures in the system. If a single fault case is identified by the

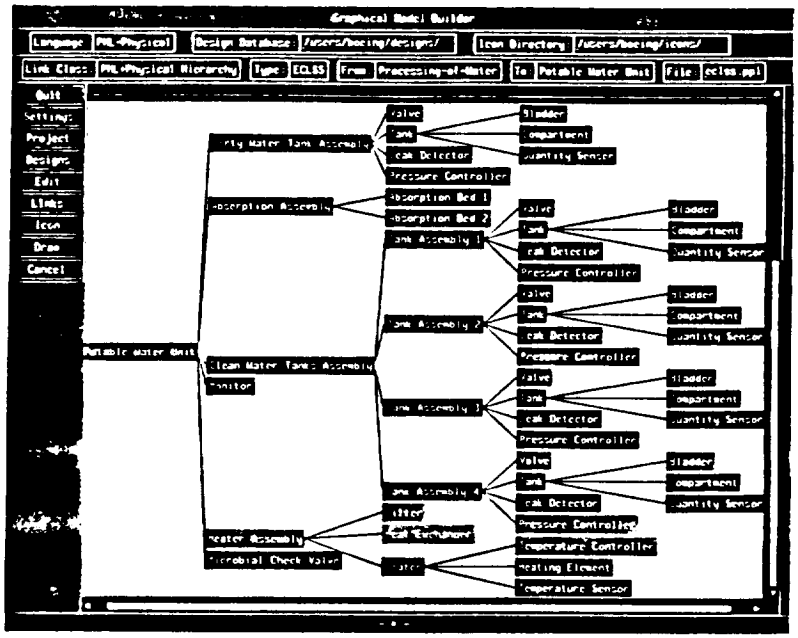

Figure 2: PWS Component Hierarchy

FCIA, the number of identified fault source candidates depends on the fault model. The primary factor is the number and allocation of alarms to failure-modes in the FPG. Since alarms are derived from sensors, the number of sensors allocated for diagnostic purposes affects the diagnostic result. If the number of sensors is low, then the number of identified fault source candidates can be high. On the other hand, if the the number of sensors are sufficient and are allocated to the right failure-modes in a FPG, the number of identified fault source candidates in a single fault case can be one. The other factor affecting the number of identified fault source candidates is the internal structure, i.e. the FPG and the component failure-mode associations, of the fault model of each process in the HFM.

PWS MODELS

The Potable Water System (PWS) of the ECLSS is decomposed from its structural aspect, resulting in a component hierarchy [5] shown in Figure 2. It is also decomposed in its functional aspect, resulting in a function hierarchy [5] shown in Figure 3.

SYSTEM DIAGNOSABILITY

Designers of modern industrial and space systems would like to use a lesser number of sensors for diagnostic purposes, in order to reduce costs. This is especially true in space systems because the total weight as well the total cost of sensors has to be reduced. Before they decide to eliminate a sensor, they would like to know the effects of its removal on the diagnostic result. Hence an approach that studies the diagnosability of a system given a particular sensor allocation is very useful to space system designers.

Some of the important terms in diagnosability studies are provided.

- **Sensor Allocation:** The number of sensors in the system, and the places in the system where they have been installed.

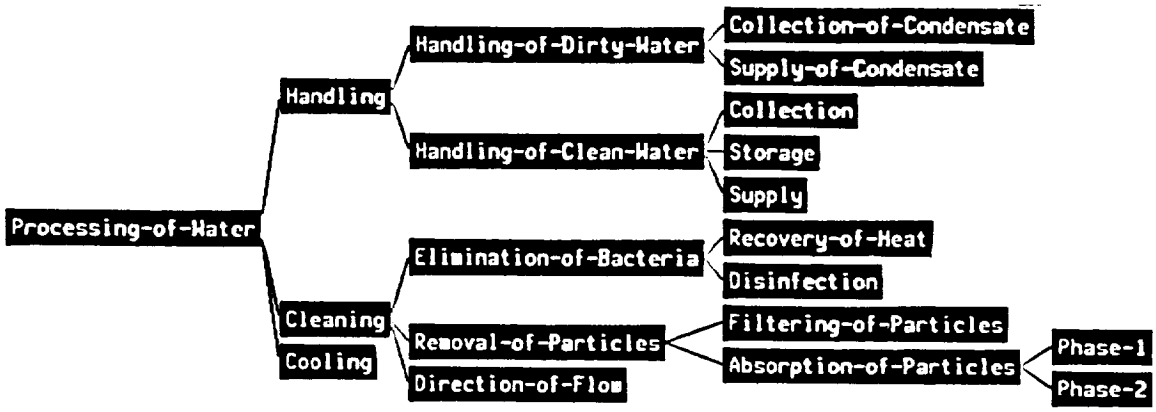

Figure 3: PWS Function Hierarchy

- **Diagnostic Result:** The set of fault source components diagnosed under no time constraints.
- **Time Constrained Diagnostic Result:** The set of fault source components diagnosed within a specific time constraint.
- **Single Component Diagnosability:** The diagnostic result when the single component in question is the fault source.
- **Multiple Component Diagnosability:** The diagnostic result when the specified multiple components are the set of fault source components.
- **Unique Diagnosability:** The diagnostic result is the same as the set of actual fault source components. In single fault cases the number of components in the diagnostic result and the actual set of fault source components is equal to one.

The single component diagnosability, multiple component diagnosability, and unique diagnosability definitions can be extended to include the case of time constrained diagnostic result.

Diagnosability Studies

A variety of studies can be performed on the system in order to determine its diagnosability. Given a particular sensor allocation, the diagnosability of components can be obtained. By eliminating a sensor from the allocation, the differences in the diagnosability of components can be determined. If the differences are minimal the designer has the option of eliminating that sensor. Finally, a study can be performed to find an optimal sensor allocation that provides unique diagnosability.

Simulation Method

The simulation method is used to demonstrate some aspects of the diagnosability studies. This method involved developing a fault simulator that simulates actual fault scenarios. The fault model of the system,

which includes the sensor allocation, serves as the internal database for the simulator. This internal database is automatically generated during the diagnostic runtime system generation phase by the diagnostic interpretor. The simulator is stand-alone program that can accept as input, a set of fault source components with their selected failed-states. The pattern of ensuing alarms is derived, and is simulated in real-time. This real-time alarm pattern serves as the input to the diagnostic process. A diagnostic result is generated on receipt of the simulated alarm pattern.

The diagnosability of any component can now be observed for any given sensor allocation. For a given sensor allocation, the fault scenario or the real-time alarm pattern with the component under question being the fault source is obtained. This real-time alarm pattern serves as the input for the diagnostic process. The generated diagnostic result is stored and compared with the diagnostic results from other sensor allocations. The effects of different sensor allocations on the diagnosability of a component can be studied in this manner.

Another use of such a simulator is to study the effects of adding or removing a sensor on the diagnostic process. Initially the designer can select a sensor of interest. The simulator determines all the components that are affected by the presence and absence of this sensor. Two fault simulations are generated for each of the affected components, one with the sensor being present and the other with the sensor being absent. The diagnosability of each component in both cases is determined on the basis of the two simulations. A statistical measure based on the diagnotic results, can then be used to determine whether or not the sensor should be retained in the system.

The simulation method is an effective first step in demonstrating the need for and effectiveness of diagnosability studies. It is quite effective in determining the diagnosability of a component. It sometimes proves useful in helping a designer decide whether to retain a sensor in the system or not. However, the process of finding the diagnostic result for all components before and after the removal of a particular sensor is very cumbersome and time consuming. The same process has to be repeated for any other sensor allocation. If the designer wants to determine an optimal sensor allocation that will achieve unique diagnosability in single fault cases, he/she has to simulate all possible sensor allocations before finding the answer. This process has an exponential time complexity because the number of possible sensor allocations can be $O(2^n)$, where n is the total number of failure-modes in the system. This complexity is clearly unacceptable for large-scale systems. An analytical method of a more manageable time complexity is definitely required for solving the problems of system diagnosability.

PWS DIAGNOSABILITY STUDY

An example that presents the effects on system diagnosability when a sensor is removed, is presented. The relevant portions of the fault model of the chosen process, Absorption-of-Particles is shown in Figure 4.

Initial Sensor Allocation

The sensor allocation for the failure-modes of the Absorption-of-Particles process and the failure-modes of its subprocesses follows:

- Sensor Allocation in Subprocess **Phase-1**.

  sudden-bad-absorption: Sensor S0, Alarm A0. *slow-bad-absorption*: Sensor S1, Alarm A1. *reverse-absorption*: Sensor S2, Alarm A2.

- Sensor Allocation in Subprocess **Phase-2**

  sudden-bad-absorption: Sensor S3, Alarm A3. *slow-bad-absorption*: Sensor S4, Alarm A4. *reverse-absorption*: Sensor S5, Alarm A5.

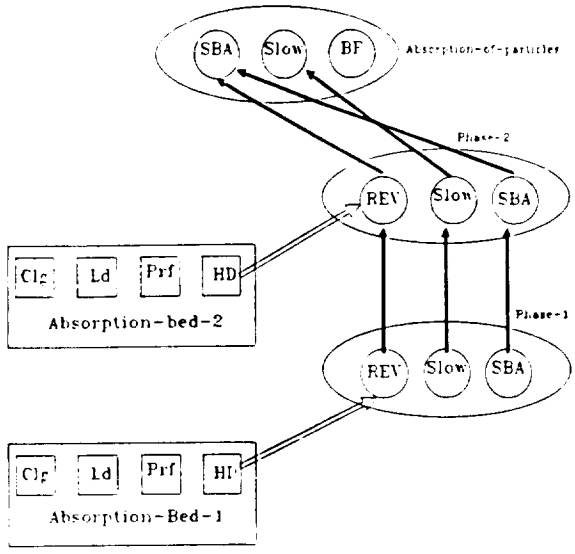

Figure 4: Absorption-of-Particles fault model

- Sensor Allocation in Process **Absorption-of-Particles**.

  sudden-bad-absorption: Sensor S6, Alarm A6. *slow-bad-absorption*: Sensor S7, Alarm A7. *bad-flow*: Sensor S8, Alarm A8.

The single component diagnosability for the two associated components when only one failed-state is simulated at a time is:

- *Absorption Bed 1:*

  Heat Damaged: Absorption Bed 1 Heat Damaged. *Loaded:* Absorption Bed 1 Loaded. *Perforated:* Absorption Bed 1 Perforated. *Clogged:* Absorption Bed 1 Clogged and Absorption Bed 2 Clogged.

- *Absorption Bed 2:*

  Heat Damaged: Absorption Bed 2 Heat Damaged. *Loaded:* Absorption Bed 2 Loaded. *Perforated:* Absorption Bed 2 Perforated. *Clogged:* Absorption Bed 2 Clogged and Absorption Bed 1 Clogged.

The explanation of the diagnostic result is provided for the cases of absorption bed 1 and 2 being in the heat damaged failed state. If the absorption bed 1 is heat damaged, the alarms generated by the simulation in order are: A2, A5, A6. The alarm A2 is associated with failure-mode reverse-absorption in the phase-1 process. There exists a failure-propagation link from this failure-mode to the reverse-absorption failure-mode in the phase-2 process. Alarm A5 is associated with the reverse-absorption failure-mode in the phase-2 process. There exists a failure-propagation link from this failure-mode to the sudden-bad-absorption failure-mode in the Absorption-of-Particles process. Alarm A6 is associated with the sudden-bad-absorption failure-mode in the Absorption-of-Particles process. The FCIA decides that alarm A2 is the primary alarm since this alarm could have caused alarms A5 and A6. The ancestor components of the failure-mode associated with the primary alarm are the initial set fault source hypothesis. In this case it is absorption bed 1 in heat damaged failed state. After ascertaining the fact that if absorption bed 1 was heat damaged the times at

which alarms A2, A5, and A6 could have been generated are not in conflict with the actual generation times, the absorption bed 1 in heat damaged state is returned by the FCIA as the diagnostic result.

If absorption bed 2 is heat damaged, the alarms generated by the simulation in order are: A5, A6. The FCIA decides that alarm A5 is the primary alarm. The possible ancestor components of the failure-mode associated with this alarm are absorption bed 1 being heat damaged and absorption bed 2 being heat damaged. However, if absorption bed 1 was heat damaged, alarm A2 would have been generated. Since this did not happen, absorption bed 1 being heat damaged is removed from the list of identified fault source components. Therefore, the final diagnostic result is absorption bed 2 being heat damaged.

Final Sensor Allocation

The sensor S2 associated with alarm A2 and attached to failure-mode reverse-absorption in the phase-1 process is removed. The resultant sensor allocation follows:

- Sensor Allocation in Subprocess **Phase-1**.

  sudden-bad-absorption: Sensor S0, Alarm A0. *slow-bad-absorption*: Sensor S1, Alarm A1. *reverse-absorption*: No sensor.

- Sensor Allocation in Subprocess **Phase-2**

  sudden-bad-absorption: Sensor S3, Alarm A3. *slow-bad-absorption*: Sensor S4, Alarm A4. *reverse-absorption*: Sensor S5, Alarm A5.

- Sensor Allocation in Process **Absorption-of-Particles**.

  sudden-bad-absorption: Sensor S6, Alarm A6. *slow-bad-absorption*: Sensor S7, Alarm A7. *bad-flow*: Sensor S8, Alarm A8.

The single component diagnosability for the two associated components is when only one failed-state is simulated at a time is:

- *Absorption Bed 1:*

  Heat Damaged: Absorption Bed 1 Heat Damaged and Absorption Bed 2 Heat Damaged. *Loaded:* Absorption Bed 1 Loaded. *Perforated:* Absorption Bed 1 Perforated. *Clogged:* Absorption Bed 1 Clogged and Absorption Bed 2 Clogged.

- *Absorption Bed 2:*

  Heat Damaged: Absorption Bed 2 Heat Damaged and Absorption Bed 1 Heat Damaged. *Loaded:* Absorption Bed 2 Loaded. *Perforated:* Absorption Bed 2 Perforated. *Clogged:* Absorption Bed 2 Clogged and Absorption Bed 1 Clogged.

A graphical tabulation of the diagnosability results in both cases of sensor allocation is shown in Figure 5.

The explanation of the diagnostic result is provided for the cases of absorption bed 1 and 2 being in the heat damaged failed state. The sensor S2 has been removed, therefore alarm A2 no longer exists, and the failure-mode reverse-absorption in the phase-1 process has no associated alarm. If either the absorption bed 1 or the absorption bed 2 was heat damaged, the alarms generated by the simulation in order are: A5, A6. The alarm A5 is diagnosed as the primary alarm. The ancestor components of this alarm are absorption bed 1 being heat damaged and absorption bed 2 being heat damaged. Since there is no alarm A2 in the fault model, the hypothesis absorption bed 1 being heat damaged has to retained. Hence if either of the two components is the fault source, the diagnostic result contains both of them.

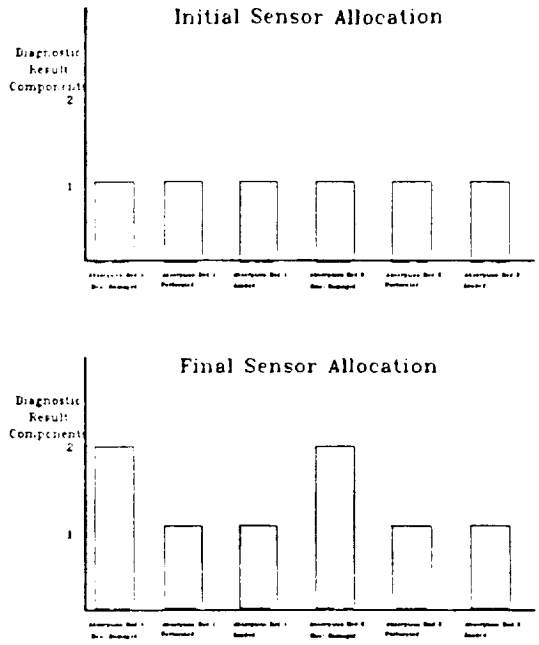

Figure 5: Diagnosability results

1 Acknowledgements

This work was supported by a grant from the BOEING Aerospace Co. Huntsville, Al. The authors would like to thank J. Ray Carnes of BOEING Computer Services for his insight, advice, and expertise. Charles Reeves, Roger Vonyouanne, and Art Brown provided the domain expertise for developing the various models.

References

[1] T. Laffey, P. Cox, J. Schmidt, S. Kao, and J. Read, *Real-Time Knowledge-Based Systems*, A.I. Magazine, Spring 1988, pp 27-45.

[2] G. Karasi, *Declarative Programming using Visual Tools*, Internal Report, Electrical Engineering, Vanderbilt University.

[3] C. Biegl, *Design and Implementation of an Execution Environment for Knowledge Based systems*, Ph.D. Dissertation, Electrical Engineering, Vanderbilt University, August 1988.

[4] S. Padalkar, G. Karsai, and J. Sztipanovits, *Graph-Based Real-Time Fault Diagnostics*, Proc. of the Fourth Conf. on A.I. for Space Applications, pp 115-123, Huntsville, AL, 1988.

[5] W. Blokland, S. Padalkar and J. Sztipanovits, *Study and Approach to Artificial Intelligence Testing: Modeling the Potable Water System of the Environmental Control And Life Support System (ECLSS)*, Vanderbilt University, 1990.